IN THE CLAIMS:

Please cancel claims 1-118 without prejudice or disclaimer, and substitute new claims 119-182 therefor as follows:

Claims 1-118 (Cancelled).

119. (New) A method for negotiating the provision of a mobile IP service between a mobile node and a server in a network, comprising the steps of:

providing an authentication protocol establishing a pass-through transport between said mobile node and said server; and

negotiating the provision of said mobile IP service via said authentication protocol over said pass-through transport.

120. (New) The method of claim 119, wherein said authentication protocol is extensible authentication protocol (EAP).

121. (New) The method of claim 120, comprising the step of selecting said transport as either of a level-2 or level-3 EAP transport.

122. (New) The method of claim 120, comprising the step of providing in said network a client node between said mobile node and said server, wherein said client node plays a pass-through role and is not involved in said negotiation.

123. (New) The method of claim 122, comprising the step of providing between said client node and said server an EAP transport selected from diameter and radius.

124. (New) The method of claim 122, comprising the step of configuring said client node as a point of attachment to said network working as an access point.

125. (New) The method of claim 122, comprising the step of configuring said client node as a point of attachment to said network working as a router.

126. (New) The method of claim 119, wherein said step of negotiating comprises at least one of:

authorizing said mobile node to use said mobile IP service;

communicating to said mobile node a set of options for use of said mobile IP service;

dynamically configuring a set of parameters required for using said mobile IP service; and

configuring further options related to said mobile IP service.

127. (New) The method of claim 120, comprising the step of routing messages for activating said mobile IP service between said mobile node and said server via said extensible authentication protocol (EAP) over said EAP transport upon at least one of said mobile node power up or connection of said mobile node to said network.

128. (New) The method of claim 119, comprising the steps of:

providing in said network a home agent for communicating with said server; and

maintaining within said home agent configuration information for providing said mobile IP service.

129. (New) The method of claim 128, comprising the step of providing an AAA backbone protocol for transferring said configuration information between said home agent and said server.

130. (New) The method of claim 119, comprising the step of performing, upon at least one of said mobile node power up or connection of said mobile node to said network, a bootstrap procedure including steps selected from:

authorizing said mobile node to use said mobile IP service,

communicating to said mobile node options for use within said mobile IP service,

configuring the parameters for use of said mobile IP service, and

configuring service options communicated to said mobile node.

131. (New) The method of claim 130, wherein said parameters comprise at least one of: a home address for use by said mobile node, the address of an associated home agent allotted thereto, and cryptographic data for bootstrapping a security association with said home agent.

132. (New) The method of claim 119, comprising the steps of:

performing said method while said mobile node is roaming within a network different from the network of its home provider; and

providing a proxy for communication between said mobile node and said server under said roaming conditions.

133. (New) The method of claim 120, comprising at least one of:

said mobile node sending a respective identifier toward said server,

setting up a transport layer security tunnel between said mobile node and said server to protect authentication information,

authenticating said mobile node with said server,

closing said EAP communication after authenticating said mobile node and negotiating said mobile IP service therefor, and

negotiating a security association between said mobile node and a respective home agent.

134. (New) The method of claim 133, comprising, in association with said authentication, the step of said mobile node and said server exchanging a set of attributes selected from attributes for authorising, negotiating and configuring said mobile IP network.

135. (New) The method of claim 133, wherein said step of negotiating said security association involves an IKE negotiation.

136. (New) The method of claim 133, wherein said authentication is based on a defined EAP method.

137. (New) The method of claim 133, wherein said authentication is SIM-CARD based.

138. (New) The method of claim 119, wherein said step of negotiating comprises the step of said mobile node sending toward said server a message comprising a set of information items selected from:

service selection information items indicating the mobile node choice to activate said mobile IP service,

service option information items, representative of the service options to be activated,

an indication of a mobile node's preferred home agent,

an indication of a mobile node's preferred home address, and

an interface identifier for use by a home agent for constructing the mobile node's home address.

139. (New) The method of claim 119, wherein said step of negotiating comprises said server selectively identifying a home agent for providing said mobile IP service.

140. (New) The method of claim 139, comprising the step of:

said server sending a home address request message to said home agent comprising an identifier for said mobile node, and

said home agent allotting a home address for said mobile node.

141. (New) The method of claim 140, wherein said step of allotting said home address comprises either generating an interface identifier or utilizing a mobile node's indicated interface identifier.

142. (New) The method of claim 140, comprising the step of said home agent performing a duplicate address detection for said home address.

143. (New) The method of claim 142, comprising, upon successful completion of said duplicate address detection, the step of said home agent preventing said home address allotted from being allocated to another user.

144. (New) The method of claim 143, comprising the steps of providing in said home agent a binding cache and registering in said binding cache a dummy entry comprising said home address and an unspecified address as a care-of address, whereby any binding update reaching said home agent does not lead to the creation of a new entry.

145. (New) The method of claim 119, comprising the steps of:

including in said network a home agent for providing said mobile IP service;

configuring said server as a key distribution centre between said mobile node and said home agent; and

sending from said server to said mobile node and said home agent cryptographic information to permit bootstrapping a security association between said mobile node and said home agent.

146. (New) The method of claim 119, comprising the steps of:

including in said network a home agent for providing said mobile IP service; and

said server sending to said home agent a home agent configuration request message comprising information items selected from:

an identifier for said mobile node,

an authorization lifetime indicating how long said mobile node is authorized to use said mobile IP service,

bootstrap information for a security association between said mobile node and said home agent, and

a set of policies for said home agent to manage said mobile node's traffic.

147. (New) The method of claim 146, comprising the step of providing in said network a home agent for communicating with said server said set of policies comprising information items representative of filtering rules to be enforced by said home agent on the mobile node traffic.

148. (New) The method of claim 120, comprising at least one of the steps of:

said server sending an authorisation message for said mobile IP service within an EAP message starting said authentication step;

upon receiving the indication from said mobile node to activate said mobile IP service, said server sending a home address request message toward a selected home agent while continuing said authentication of said mobile node; and

said server continuing said authentication procedure of said mobile node by completing configuration of a respective home agent for providing said mobile IP service before completing said authentication procedure.

149. (New) The method of claim 120, comprising the steps of:

selecting said network as a network using a respective authentication method other than EAP; and

using said EAP transport for said step of negotiating, while providing authentication by said respective authentication method other than EAP.

150. (New) The method of claim 149, comprising the steps of:

selecting said network as a cellular network including a GGSN node; and

allotting to said mobile node an IP address by activating a PDP context, whereby a direct communication channel is established between said mobile node and said GGSN node.

151. (New) A system for negotiating the provision of a mobile IP service between a mobile node and a server in a network, comprising an authentication protocol for establishing a pass-through transport between said mobile node and said server and being configured for negotiating the provision of said mobile IP service via said authentication protocol over said pass-through transport.

152. (New) The system of claim 151, wherein said authentication protocol is extensible authentication protocol (EAP).

153. (New) The system of claim 152, wherein said transport is either of a level-2 or level-3 EAP transport.

154. (New) The system of claim 152, comprising a client node between said mobile node and said server, wherein said client node plays a pass-through role and is not involved in said negotiation.

155. (New) The system of claim 154, comprising between said client node and said server, an EAP transport selected from diameter and radius.

156. (New) The system of claim 154, wherein said client node is a point of attachment to said network configured as an access point.

157. (New) The system of claim 154, wherein said client node is a point of attachment to said network configured as a router.

158. (New) The system of claim 151, wherein said system is configured for performing at least one of:

authorizing said mobile node to use said mobile IP service,

communicating to said mobile node a set of options for use of said mobile IP service,

dynamically configuring a set of parameters required for using said mobile IP service, and

configuring further options related to said mobile IP service.

159. (New) The system of claim 152, wherein said system is configured for routing messages for activating said mobile IP service between said mobile node and said server via said extensible authentication protocol (EAP) over said EAP transport

upon at least one of said mobile node power up or connection of said mobile node to said network.

160. (New) The system of claim 151, comprising a home agent for communicating with said server and maintaining configuration information for providing said mobile IP service.

161. (New) The system of claim 160, comprising an AAA backbone protocol for transferring said configuration information between said home agent and said server.

162. (New) The system of claim 151, wherein said system is configured for performing, upon at least one of said mobile node power up or connection of said mobile node to said network, a bootstrap procedure comprising steps selected from:

authorizing said mobile node to use said mobile IP service,

communicating to said mobile node options for use within said mobile IP service,

configuring the parameters for use of said mobile IP service, and

configuring service options communicated to said mobile node.

163. (New) The system of claim 162, wherein said parameters comprise at least one of: a home address for use by said mobile node, the address of an associated home agent allotted thereto, and cryptographic data for bootstrapping a security association with said home agent.

164. (New) The system of claim 151, comprising a proxy for communication between said mobile node and said server while said mobile node is roaming with a network different from the network of its home provider.

165. (New) The system of claim 152, comprising at least one of:

an EAP communication transport between said mobile node and said server, whereby said mobile node is able to send a respective identifier toward said server;

a transport layer security tunnel between said mobile node and said server to protect authentication information;

an authentication function for authenticating said mobile node with said server;

an EAP communication closing function for closing said EAP communication after authenticating said mobile node and negotiating said mobile IP service therefor; and

a security association between said mobile node and a respective home agent.

166. (New) The system of claim 165, comprising, in association with said authentication, a set of attributes to be exchanged between said mobile node and said server, said set of attributes selected from attributes for authorising, negotiating and configuring said mobile IP network.

167. (New) The system of claim 165, wherein said security association is based on an IKE negotiation.

168. (New) The system of claim 165, wherein said authentication is based on a defined EAP system.

169. (New) The system of claim 165, wherein said authentication is SIM-CARD based.

170. (New) The system of claim 151, wherein said mobile node is configured for sending toward said server a message comprising a set of information items selected from:

service selection information items indicating the mobile node choice to activate said mobile IP service,

service option information items, representative of the service options to be activated,

an indication of a mobile node's preferred home agent,

an indication of a mobile node's preferred home address, and

an interface identifier for use by a home agent for constructing the mobile node's home address.

171. (New) The system of claim 151, wherein said server is configured for selectively identifying a home agent for providing said mobile IP service.

172. (New) The system of claim 171, wherein

said server is configured for sending a home address request message to said home agent comprising an identifier for said mobile node, and

said home agent is configured for allotting a home address to said mobile node.

173. (New) The system of claim 172, wherein said home agent is configured for allotting said home address either by generating an interface identifier or by utilizing a mobile node's indicated interface identifier.

174. (New) The system of claim 172, wherein said home agent is configured for performing a duplicate address detection for said home address.

175. (New) The system of claim 174, wherein said home agent is configured for preventing said home address allotted from being allocated to another user upon successful completion of said duplicate address detection.

176. (New) The system of claim 175, wherein said home agent has a binding cache and is configured for registering in said binding cache a dummy entry comprising said home address and an unspecified address as a care-of address whereby any binding update reaching said home agent does not lead to the creation of a new entry.

177. (New) The system of claim 151, comprising:

a home agent for providing said mobile IP service;

said server configured as a key distribution centre between said mobile node and said home agent, for sending to said mobile node and said home agent cryptographic information to permit bootstrapping a security association between said mobile node and said home agent.

178. (New) The system of claim 151, comprising:

a home agent for providing said mobile IP service, said server being configured for sending to said home agent a home agent configuration request message comprising information items selected from:

an identifier for said mobile node,

an authorisation lifetime indicating how long said mobile node is authorized to use said mobile IP service,

bootstrap information for a security association between said mobile node and said home agent, and

a set of policies for said home agent to manage said mobile node's traffic.

179. (New) The system of claim 178, wherein said network comprises a home agent for communicating with said server, said set of policies comprising information

items representative of filtering rules to be enforced by said home agent on the mobile node traffic.

180. (New) The system of claim 152, configured for performing at least one of the steps of:

said server sending an authorisation message for said mobile IP service within an EAP message starting said authentication step,

upon receiving the indication from said mobile node to activate said mobile IP service, said server sending a home address request message toward a selected home agent while continuing said authentication of said mobile node, and

said server continuing said authentication procedure of said mobile node by completing configuration of a respective home agent for providing said mobile IP service before completing said authentication procedure.

181. (New) The system of claim 152, wherein said network is a network having a respective authentication function other than EAP and said system is configured for using said EAP transport for said step of negotiating, while providing authentication by said respective authentication function other than EAP.

182. (New) The system of claim 181, wherein said network is a cellular network comprising a GGSN node, and the system is configured for allotting to said mobile node an IP address by activating a PDP context, whereby a direct communication channel is established between said mobile node and said GGSN node.